Fulfilling a Crucial Role

National Intelligence Support Teams

James M. Lose

"One means of providing timely, tailored national intelligence support to deployed forces is through a NIST."

In the early and mid-1990s, even as the US Department of Defense worked to reduce its Cold War-size budgets, it found its military forces becoming embroiled in numerous "low-intensity conflicts" around the world.[1] The global situation that President Bush characterized as the "New World Order" soon proved to be a world in *disorder*. New threats have emerged that pose new challenges for the Intelligence Community (IC). Accordingly, the IC has employed several recent innovations to meet these new tasks. One such innovation that has proven to be invaluable during recent US military operations is the National Intelligence Support Team (NIST).[2]

The National Security Environment

In *A National Security Strategy of Engagement and Enlargement*, President Clinton describes the new dangers to our nation's security as being more varied than ever before. The emerging threats to US security he addresses include regional aggressions; the spread of weapons of mass destruction; ethnic, religious, and national rivalries; international terrorism; transnational drug trafficking; and international organized crime. His strategy for responding to these threats states that, in order to advance its national objectives, the United States must continue to be engaged in the world through its leadership, and its national security strategy must be based "on enlarging the world community of secure, democratic, and free market nations."[3] The military is one foreign policy tool available to achieve the administration's national objectives.

Since the fall of the Soviet Union in 1991, the likelihood that the United States will be engaged in a full-scale conflict has decreased to the extent that few leaders in the US Government believe that, other than on the Korean Peninsula or in the Middle East, US forces will be required to fight a war in the next 15 to 20 years. The possibility of the US military becoming involved in other crises abroad, however, has risen significantly as the nation seeks to advance its interests through the policies of engagement and enlargement.

The unique unconventional nature of these new threats compels the commander to rely more heavily on his intelligence officer than he may deem necessary in more conventional combat operations. With this increased reliance on intelligence, the intelligence officers at the theater and tactical levels have looked to the national IC for support to fill the commander's information shortfalls. Consequently, the IC has sought to provide support to the tactical commander with historically unprecedented vigor. One means of providing timely, tailored national intelligence support to deployed forces is through a NIST.

Background, Mission, and Functions

"Based on the lessons learned from Operations DESERT SHIELD and DESERT STORM, all national-level

James M. Lose is a Captain in the US Marine Corps.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2000		**00-00-1999 to 00-00-2000**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
National Intelligence Support Teams	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Center for the Study of Intelligence,Central Intelligence Agency,Washington,DC,20505**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Studies in Intelligence. Volume 43, No. 3, Winter 1999-2000

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**10**	

agencies combined their separate deployed intelligence support cells into one NIST."[4] A NIST normally is composed of personnel from DIA, NSA, NIMA, and the CIA who are deployed upon request by the military commander to facilitate the flow of timely all-source intelligence between a Joint Task Force (JTF) and Washington, DC, during crises or contingency operations.[5] Teams are specifically configured to meet the needs of the deployed commander. Since their inception, NISTs have provided intelligence support to Operations PROVIDE RELIEF (Kenya), SOUTHERN WATCH (Saudi Arabia), RESTORE HOPE (Somalia), DENY FLIGHT and PROVIDE PROMISE (the Balkans), UPHOLD DEMOCRACY (Haiti), JOINT ENDEAVOR (Bosnia), GUARDIAN ASSISTANCE and GUARDIAN RETRIEVAL (Zaire), JOINT GUARD and JOINT FORGE (Bosnia), SHINING PRESENCE (Israel), JOINT GUARDIAN (Kosovo), and NOBLE ANVIL (Albania).

The NIST concept is designed to create a dynamic flow of intelligence to and from the JTF operational area.[6] A NIST is able to provide unique intelligence support to a JTF commander in several ways. First, and most frequently, the NIST provides "reach-back" to national IC agencies and a thorough knowledge of each agency's resources and capabilities that normally does not exist at the JTF level. Team members provide a direct agency liaison for the JTF, and they have an excellent understanding of where to go in their parent agency to obtain the best support for the commanders' priority intelligence requirements. This reach-back capability usually is accomplished informally, with team members either

"The NIST concept is designed to create a dynamic flow of intelligence to and from a Joint Task Force operational area. A NIST can provide unique intelligence support to a JTF commander."

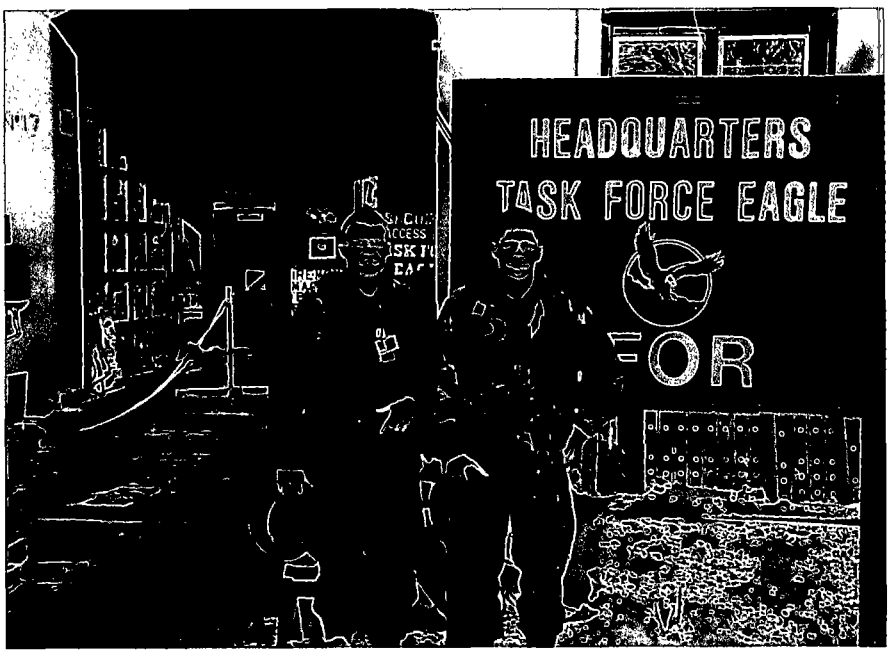
requesting encyclopedic intelligence or querying analytic resources with quick questions that do not require new tasking of national assets. The NISTs can also facilitate the flow of information to and from the Area of Responsibility via e-mail or video teleconference (VTC).[7]

The direct link to Washington is the most controversial of a NIST's roles, and it may sometimes be viewed by the JTF J2 as a two-edged sword. The reach-back capability that JTF J2s desire often becomes a *reach-forward* for national agencies that want on-the-scene reporting, information on operational issues, details for briefings, or other information directly from the NIST. The way in which queries from Washington-based national IC agencies (often referred to in the field simply as "National") are handled determines whether the supported command will begin to view the NIST as the National Intelligence *Spy* Team. My first NIST deployment to Bosnia provides one example of how this issue can be managed.

Shortly after the NIST arrived in Tuzla in December 1995, questions from National became an almost daily occurrence. Our team discussed this development with the Task Force Eagle (TFE) G2 and explained to her that, no matter what we did, the requests for information (RFIs) from National would surely continue. Nevertheless, the team assured her that we would clear our responses either with her or one of the watch officers and that no NIST member would pass information back to National that pertained to ongoing or future operations. This arrangement appeased the briefers in Washington, since they received intelligence from someone on the scene, and the G2 was satisfied with the agreement not to pass operational details via intelligence channels.

One of the best examples of the reach-back capability was NIST-Tuzla's early successes in communicating Task Force Eagle's essential elements of information (EEI) to the national IC. At the outset of Operation JOINT ENDEAVOR, although thousands of US troops had begun deploying to Bosnia, the intelligence production from IC agencies seemed to focus on briefings emanating from inside the Beltway and not on the intelligence needs of the tactical commander. This frustrated the TFE G2. After gaining her approval, NIST-Tuzla sent TFE's EEIs to the various Balkans-oriented intelligence task forces throughout the IC.

In addition, once the production focus began to shift and tactical intelligence requirements gained attention, NIST-Tuzla coordinated with theater and national intelligence organizations, various US Army (Europe) units, and the other NISTs in-theater to host weekly analyst-to-analyst VTC chats to answer common questions and have analysts at all levels interact in an informal setting. As a testament to its value, the



NIST members in front of Task Force Eagle Headquarters (author is on right). March 1996. Photo courtesy of the author.

"Balkans analysts' VTC," as it became known, has taken place on a weekly basis since January 1996 and is hosted by the Director of Central Intelligence's Balkan Task Force.

A second unique aspect of a NIST's intelligence support is that it provides a threat warning capacity to the JTF and enhances the commander's overall force protection capability. The NSA element of a NIST usually contains a few personnel from the National Security Operations Center's Special Support Activity. They provide a small mobile SATCOM system that allows the JTF commander to receive threat warning broadcasts from NSA Headquarters that pertain to his operating area. The NSA element also receives prioritized near-real-time intelligence messages over its computer systems, which connect directly into the NSA network in Ft. Meade, Maryland.[8]

Before the deployment to Tuzla, the TFE commander requested that the NIST, which had been pre-positioned in Germany to join the 1st Armored Division, provide a threat warning capability for forward-deployed units that were involved with the Sava River crossing into Bosnia. With less than an hour's notice, a two-person team from the NIST's NSA element was ready for deployment.

Third, a NIST offers several products from each of its parent agencies that may otherwise be unavailable to a JTF. These products may carry classifications that no JTF communications systems are cleared to handle but that a NIST is able to disseminate via its agency-only systems. Furthermore, certain daily publications accessible to a NIST can offer unique insight into the intelligence products that the Chairman of the Joint Chiefs of Staff (CJCS) and the Secretary of Defense receive, but which are accessible to few others. For example, DIA's former Yugoslavia Intelligence Task Force may prepare a point paper or desk note for the Joint Staff J2 in response to a question the Chairman may have about the situation in Bosnia. The NIST can request and disseminate this product so that the JTF commander and the J2 are aware of the questions that CJCS has about their operation. By doing so, the NIST may potentially assist in reconciling conflicting intelligence reports or in correcting misreporting.[9]

Fourth, a NIST enables a JTF commander to submit RFIs that require an answer from the national IC within 24 hours or less. Elements of the NIST accomplish this by communicating either with the National Military Joint Intelligence Center, which is located with the National Military Command Center in the Pentagon and is the national clearing house for all RFIs, or with each element's parent organization.[10] In those instances when direct connectivity to national agencies is essential, the NIST will coordinate with the intelligence center of the supported theater to avoid duplication of effort and ensure that national assets are not tasked when the theater could have answered the JTF's RFI.

Lessons Learned From Haiti and Bosnia

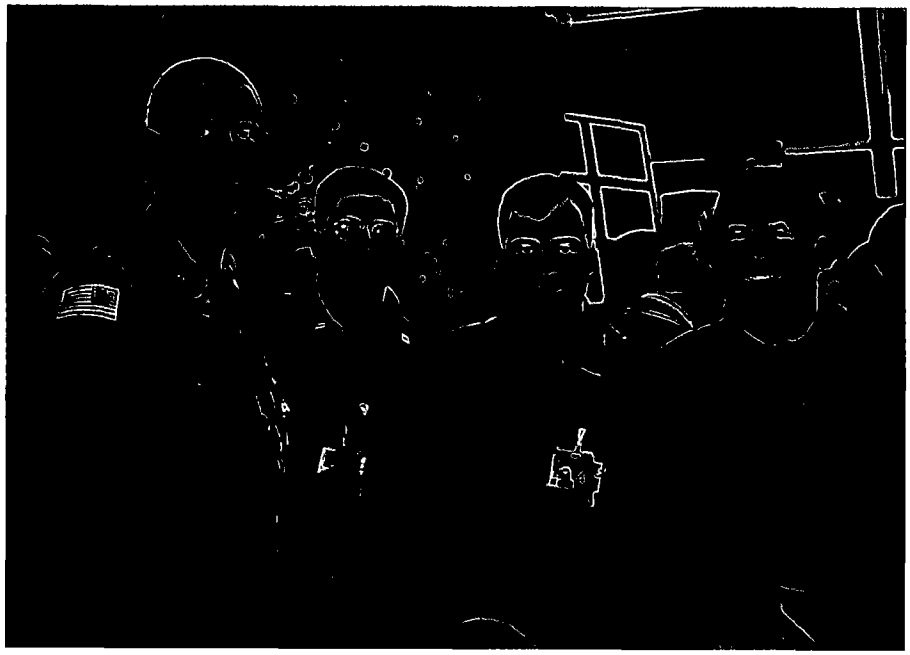
Two major operations in which NISTs participated—Operations UPHOLD DEMOCRACY in Haiti and JOINT ENDEAVOR in Bosnia—provide examples of areas in the NIST program where support to

future crisis or contingency operations could be improved. A total of nine separate NISTs provided support to both peacekeeping operations in two separate Unified Commands.

In Haiti, the mission for the combined military force, under the operational control of US Atlantic Command (USACOM), was to establish and maintain a secure government in order to facilitate the return and proper functioning of the elected Government of Haiti.[11] Early on, USACOM requested national intelligence support, and, in the end, NISTs were deployed aboard the USS Mount Whitney, the USS Wasp, and to the JTF Joint Intelligence Center in Port-au-Prince. Many lessons from the NISTs and the supported commanders proved to be beneficial when planning support to future operations:

- The first lesson is that early coordination between the NIST and the supported command is critical. During the pre-deployment phase of the operation, the NIST can pre-position its equipment, conduct necessary training, and coordinate its roles and responsibilities with the JTF J2. For Haiti, the NIST was not "read in" as to when D-Day would occur and was unable to plan effectively.

- Second, the NIST chief has to be briefed on the Operations Plan in order to prepare the team for deployment and more effectively coordinate national intelligence support. The NIST chief has to maintain strict operational security and avoid passing any operational details to the Pentagon or other Washington sanctums.



NIST and Task Force Eagle personnel with Senator John McCain (on right) during a Congressional visit to Tuzla, Bosnia. February 1996. Photo courtesy of the author.

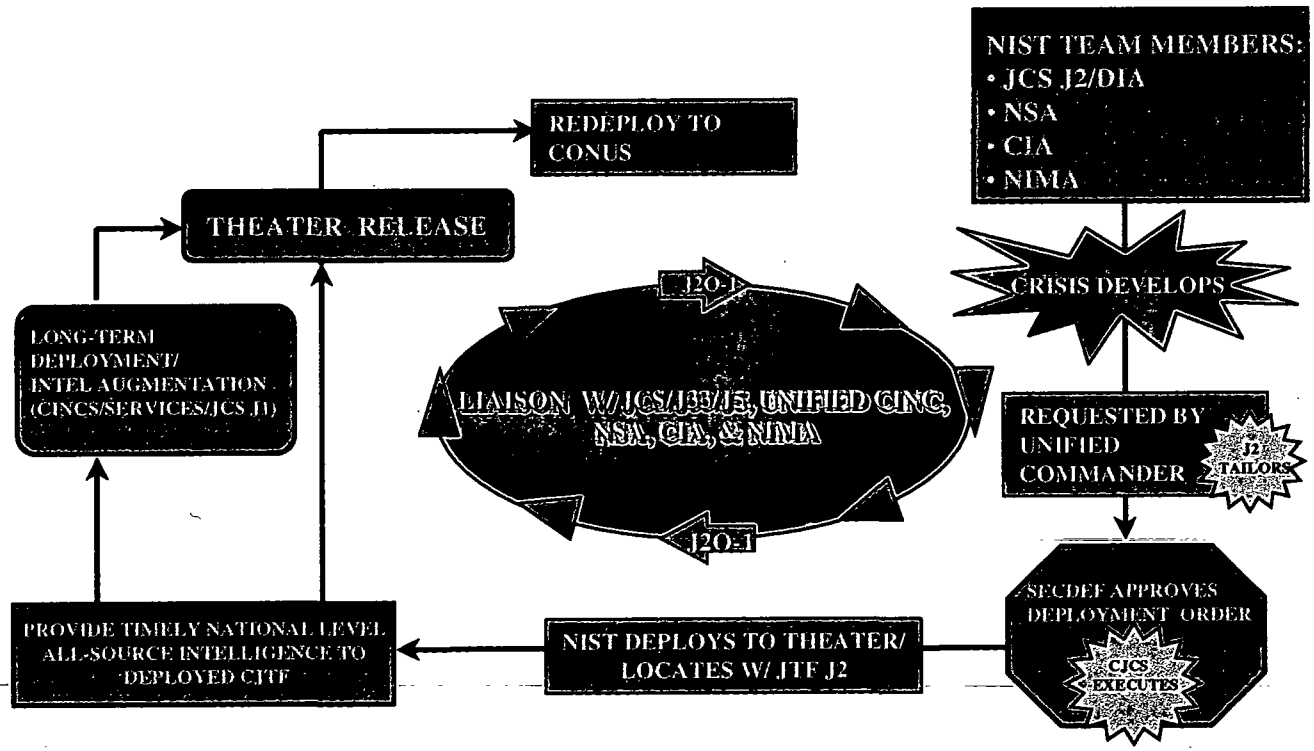
- Third, the NIST's liaison with—and coordination between—HUMINT collectors in-country and their parent organizations in Washington proved essential to operating in an environment like that encountered by US forces in Haiti. Information from HUMINT sources was highly valuable, and collection from national assets was tailored to the J2's Priority Intelligence Requirements.

- Fourth, the NIST must be located with the JTF JIC if it is to provide the best possible support to the JTF J2. This took place eventually in Operation UPHOLD DEMOCRACY, and it was considered an essential "lesson learned" for future contingencies.[12]

In supporting this complex peacekeeping operation, the reach-back that the NIST provided to Washington kept the various intelligence headquarters informed about JTF operational activities in order to cue national collection resources. On D-Day, the NIST contingent arrived in-country and rapidly established connectivity with the IC. As the operation progressed successfully, NIST support decreased quickly; it was eventually reduced to one individual before being withdrawn entirely in early 1995. This last point apparently was lost on those who managed NIST support to the next major deployment of US forces, Operation JOINT ENDEAVOR—now JOINT FORGE.

The mission of the multinational, NATO-led Implementation Force (IFOR), which conducted Operation JOINT ENDEAVOR (OJE) in Bosnia, was to patrol the Zone of Separation (as prescribed by the Dayton accords) in order to separate the

NIST Deployment Cycle



711171-7

former warring factions and help create a climate for peace. After more than four years of war in Bosnia among three ethnically divided and heavily armed adversaries, OJE began in December 1995. At one time, NIST-Naples supported the Commander-in-Chief Allied Forces Southern European Command (CINCSOUTH) in Operation PROVIDE PROMISE, while NIST-Vicenza supported NATO's Combined Air Operations Center and the air operations over the Balkans, Operation DENY FLIGHT.

Two months before the start of OJE, at the request of the CINC, NIST representatives began preparing for the deployment of two additional teams to the theater. NIST-Tuzla would support the Commander of Task Force Eagle and be located in the Multinational Division North with the US Army's 1st Armored Division G2, and NIST-ARRC would support the Commander, Allied Command Element, Rapid Reaction Corps (ARRC) and be located with the US National Intelligence Cell in Ilidza, a suburb of Sarajevo. In January 1996, two more NISTs were established: NIST-IFOR supported the IFOR Commander at his headquarters in the American Embassy compound in Sarajevo. NIST-Hungary supported the Commander, US Army Europe (Forward) in Tazsar. Thus, six NISTs supported OJE from January to December 1996.

The deployment of six teams in Bosnia for about a year duplicated intelligence efforts, reduced national agencies' capabilities to provide support in other potential crises, and depleted valuable, limited intelligence resources, including personnel and sophisticated equipment.[13] The

"NISTs deployed for an extended period inevitably become *intelligence augmentation* instead of their intended role as *crisis support.*"

design of the program is for NISTs to deploy for short periods to provide direct intelligence connectivity between a JTF and the national IC. Once a potential crisis begins to develop, the NIST program office in the Pentagon should start its deployment planning cycle by identifying qualified personnel from each of the member agencies and preparing the team's equipment.

If a "warning order" is published and time permits, the team chief may travel briefly to the supported command to conduct liaison and to prestage equipment that has to be palletized. If the CJCS issues a "Deployment Order," depending on the command's requirements, a lightly tailored NIST consisting of only enough individuals and equipment to operate the team and to meet the commander's needs (in essence, "bare bones" computer and communications support) will deploy to the theater.

After several weeks, if the crisis is not resolved, additional capabilities (such as larger communications systems with broader bandwidth capacity) can be deployed to the region. At D+90 days, the supported command should reevaluate its intelligence requirements and bring the NIST back to the United States, request the NIST for an additional 90 days, or coordinate with the theater intelligence center to ask for national support in the form of personnel augmentation or liaison officers.

This leads to a second lesson learned: NISTs deployed for an extended period inevitably become *intelligence augmentation* instead of fulfilling their intended role as *crisis support* teams. For example, the team may be used as a "bodysnatch" for non-NIST tasks, such as leading the JTF's ground order-of-battle cell, single-source SIGINT section, and so forth. In the case of NIST-Hungary, by Fall 1996 the analysts who were deployed to NIST-Hungary were actually submitting more RFIs on the situation in Zaire than on the Balkans.

Similarly, the NISTs in Naples and Vicenza were deployed for about five years. The last NATO airstrikes in Bosnia took place in 1995. CINCSOUTH, the commander whom NIST-Naples supported, relinquished command of the mission when NATO's IFOR became SFOR (Stabilization Force) in December 1996. Even though CINCSOUTH had no command over troops in Bosnia, it retained a NIST until 1997.

It is difficult to believe that the intelligence operations in Bosnia would have been compromised significantly if both NISTs in Italy had been closed in 1996. The fact that the teams continued to exist, even after the operational tempo slowed dramatically, lends credence to the charge that the NIST can serve as a convenient bypass of theater intelligence centers. A NIST is intended to provide direct access back to Washington only in emergency situations. It is not designed as a remedy for theater intelligence shortfalls.[14] After 90 to 180 days of a NIST's deployment, the theater intelligence architecture

should be prepared to replace NIST capabilities, which may include asking Washington for national agency liaison officers, if necessary. A NIST should not be used as a "cover" for permanent deficiencies in the intelligence support structure of a unified command.

Finally, another lesson learned, which applies to both Operations UPHOLD DEMOCRACY and JOINT ENDEAVOR, is that an Instruction issued by the Joint Chiefs of Staff (called a CJCSI) on the NIST should be written to replace the current NIST Concept of Operations. For this document to have credibility with JTF commanders and J2s, it needs to be signed by the Chairman of the JCS and each of the CINCs. Such an Instruction is likely to be the one means for ending disputes between theater and national intelligence centers over the management of the RFI process, and would prevent NISTs from being used as augmentation.

Suggested Improvements

Based on the lessons learned from NIST deployments to Haiti and Bosnia, certain adaptations of the program need to be enacted. Below I offer several recommendations for enhancing a NIST's overall capabilities and support to crisis operations, while at the same time preventing future deployments from lasting several years.[15]

Some IC officials would argue that it is time the NIST's mission be changed. If it is augmentation or enhanced communications that commanders want, then the reasoning is that national agencies should provide

"A NIST should not be used as an easy panacea requested by the theaters to cure all their intelligence ills."

them. Who from National would tell a CINC what the commander needs to handle a crisis in his own theater? While no one would argue that an augmentation of regional intelligence analysts or of communications equipment has to be requested by the appropriate means, the NIST is not that means. Equipment, personnel, and funds are becoming too scarce to provide a NIST to support every echelon of command in every theater hotspot. Furthermore, the readiness of the program to respond to bona fide crises suffers (lack of ability to train new personnel, wear and tear on equipment, and so forth). When six NISTs were deployed in support of the peacekeeping mission in Bosnia, one can only imagine what it would have been like if Iraq invaded Kuwait again.[16]

A NIST, in short, should not be used as an easy panacea requested by the theaters to cure all their intelligence ills. The NIST's mission has to remain that of supporting crisis or contingency operations. All other requirements for national intelligence support should be handled by other means.

Instructions and Memoranda

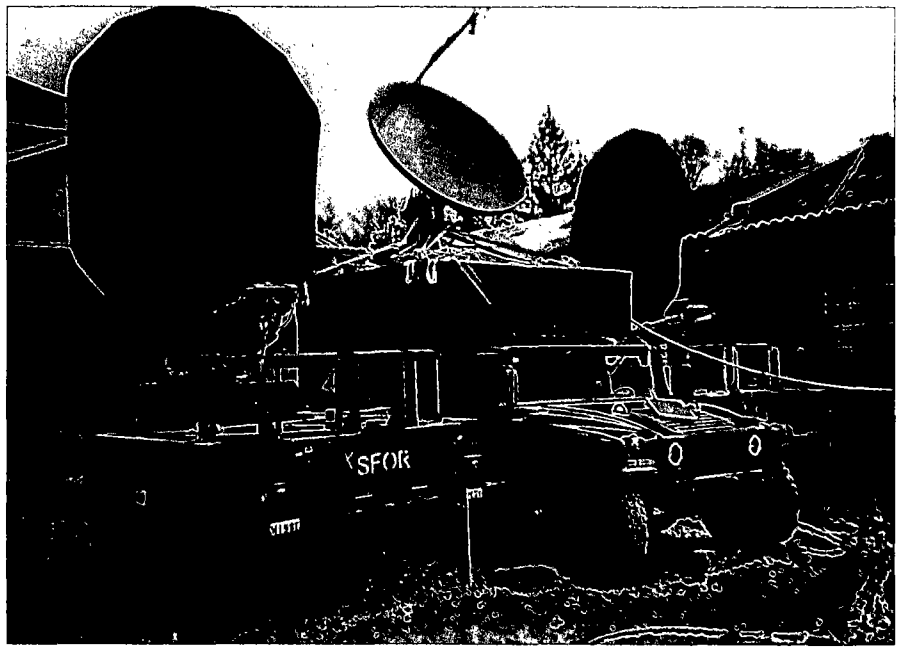
NIST doctrine should be solidified in a CJCSI, which should clearly define a NIST's mission and responsibilities and specify a maximum length of time for a NIST deployment, such as 90 to 180 days. To paraphrase one intelligence scholar and author, a crisis is only a crisis for a few weeks.[17] Following that logic, if a NIST is deployed only in support of a crisis, then the length of most deployments should be measured in weeks or months. Nevertheless, a mechanism has to be put in place to allow extension of deployments in extreme cases, and a restriction should be placed on the number of extensions the theaters can request. Until a CJCSI is signed and published, the intelligence agencies involved in the NIST program, the theater intelligence centers, and future JTF commanders are unlikely to benefit from the lessons of the Haiti and Bosnia deployments.

One doctrinal matter that has recently been resolved pertains to the Memorandum of Agreement (MOA) among the agencies involved in the program. The original MOA, written in 1993, had become outdated. With the creation of NIMA in 1996, the NIST membership has increased from the original three agencies to include NIMA. The MOA has been updated to reflect this change.

The new document should have included a specific requirement for the member agencies to send area experts familiar with the region where the crisis has occurred. Too often, agency managers keep such specialists inside the Beltway to brief policymakers, rather than deploy them forward with a NIST to the JTF. There is validity to the argument that sometimes there are too few analysts to spare to send one with a NIST. Further, analysts who are deployed for an extended period lose their *national* perspective; they may become too focused on the minutia of the situation and lose their broader outlook.

Nonetheless, it seems a small price to pay for the advantages of allowing an analyst to develop an on-the-ground situational awareness and a keen understanding of what kind of intelligence support the tactical commander requires. One CIA analyst assigned to a NIST at the beginning of an operation possessed such a high degree of acumen and area expertise that he proved to be the team's greatest asset. He routinely rounded up the JTF analysts, many of whom had little or no background in the region, to focus their analyses on the pertinent issues.

This analyst gained an invaluable appreciation for what the military customer requires, something that cannot be achieved from a desk in Langley. For this reason, the MOA should stipulate that regional analysts will deploy forward with the NIST, at least at the onset of a crisis. To entice qualified members, NIST deployments should continue to be seen as career-enhancing and be made as attractive as possible to potential volunteers.



NIST communications equipment, February 1998. Photo courtesy of the author.

Educational Program

To ensure that NISTs are used according to joint doctrine, an educational program is required. The NIST program management office should conduct frequent visits to each of the Unified and sub-Unified Commands to train the theaters on the program. In addition, it should participate in theater exercises more often by deploying smaller teams to limit cost. During the exercises, the team could demonstrate various functions by managing time-sensitive RFIs, providing unique intelligence products, and so forth. Another educational practice that should be developed is hosting quarterly VTCs with each CINC's intelligence center to discuss and review proposed NIST support in crises and to exercises in each command.

Technical Capabilities

A final recommendation, based on technological advances in the IC, is that the NIST program should seek to adopt cutting-edge communications and computer technology in order to enhance the capabilities it brings to "the fight." In the past, NISTs brought with them computer and communications systems with which personnel in the commands were generally unfamiliar, such as the Joint Deployable Intelligence Support System (JDISS) and INMARSAT mobile satellite communications terminals. This technology is now more than five years old; most intelligence analysts are well acquainted with JDISS, and the supported commands have their own INMARSAT capability. The NIST program should strive to adopt commercial off-the-shelf systems that are smaller, more rugged, and less expensive to operate. For instance, the SATCOM system that provides the broadest bandwidth possible with the smallest satellite dish and least expensive fees is the ideal.

In his remarks to a CIA audience regarding intelligence support to the humanitarian assistance operation in Somalia, Gen. Anthony Zinni, USMC, warned of the pitfalls of "stovepipe" reporting.[18] Using a common communications path is an area in which NIST performance has improved during the last several deployments. Previously, when NISTs deployed, member agencies were unable to use the same communications path. For security reasons,

some agencies hesitated to use the Joint Worldwide Intelligence Communications System (JWICS), the TOP SECRET compartmented secure intelligence network managed by DIA. Now, however, the capability exists for information on this system to be double encrypted as it moves through the JWICS. This allows all the agencies of the NIST to use one common communications platform, thereby reducing the scope of the NIST's deployable equipment by thousands of pounds and reducing the number of personnel needed to operate the various communications systems from each agency.[19]

Another technological advance the NIST should embrace is the Joint Intelligence Virtual Architecture (JIVA) initiative and the collaborative environment it espouses. JIVA allows intelligence specialists from around the world to work together on specific issues using commercial software. Using JIVA and its collaborative technology, the NIST could gain access to broader and deeper analytic resources, while maintaining a smaller footprint at the deployed location. JIVA-related innovations provide analysts with an environment in which they can exchange ideas, similar to the analysts' VTC, except with less bandwidth. While these recommendations are not critical to the overall success of the program, they would allow the NIST to hone the support it provides during future deployments.

Reasonable Cost

The benefit of implementing these recommendations far exceeds the cost. Fiscally, the NIST program office would need to allocate additional funding for more frequent visits to the CINCs and for acquiring more state-of-the art systems. Because the NIST's annual budget already includes travel expenses and equipment upgrades, a slight increase in expenditures should be feasible. The greatest cost would be in personnel hours—primarily the time it takes to publish a CJCSI. A goal of one year, from the first draft to publication, should be established to complete the project. Again, when compared to the expense of the deviations from doctrine (six NISTs deployed for more than a year supporting the same operation), the cost of doctrinal updates is minimal.

A Continuing Role

The question of whether the NIST program has outlived its utility is one that has been raised after each major deployment. It seems fitting that after seven years of operations and some 1200 intelligence and communications professionals have been deployed, the NIST program should undergo the scrutiny of an exhaustive review process. The lessons of the deployment to Haiti were incorporated and improved on for the NIST deployment to Bosnia. But the lessons from OJE, the first mission to Bosnia, and from its current operations in JOINT GUARD and SOUTHERN WATCH need to be enshrined in joint doctrine.

From its inception, the NIST program has taken the lead in providing tailored and timely national intelligence support to US forces deployed in overseas crises. As long as intelligence gaps are perceived to exist between the national and the tactical levels, the NIST will continue to have a critical mission to fulfill. In fact, with the increased threats to US national security, the NIST could be called on more frequently in the next decade than it was during the previous one.

NOTES

1. A partial listing of low-intensity conflicts includes: combating terrorism; exclusion zone operations; ensuring freedom of navigation; noncombatant evacuation operations; recovery operations; show of force; truce keeping (or peacekeeping); and support and assistance operations such as arms control support, domestic support, foreign humanitarian assistance, insurgency support, nation assistance, and support to counterdrug operations. Aryea Gottlieb and Ann E. Story, "Beyond the Range of Military Operations," *Joint Forces Quarterly*, Autumn 1995, p. 103.

2. From 1995 to the present, the author has worked in DIA, Directorate for Intelligence, J2, Deputy Directorate for Crisis Operations, NIST Division. He deployed as the DIA Element Leader with the first NIST into Bosnia and Herzegovina (NIST-Tuzla) in support of Operation JOINT ENDEAVOR, and served as the Chief of the NIST supporting Operation DELIBERATE GUARD in Vicenza, Italy.

3. *A National Security Strategy of Engagement and Enlargement*, the White House, February 1996, pp. 2-3, p. 12.

4. *Concept of Operations for the National Intelligence Support Team*, Washington, DC; DIA, 22 March 1995, p. 1.

5. JCS, Joint Pub 2-02, *National Intelligence Support to Joint Operations* (Final Coordination Draft); Washington, DC; GPO, November 1997, p. V-6.

6. *Concept of Operations*, p. 3.

7. JCS, J2 NIST briefing, "The National Intelligence Support Team Brief," *Intelink,* URL: <http:www.dia.ic.gov/intel/j2/j2o/j2o1/brief/sld009.html>. Accessed 29 April 1998.

8. "The National Intelligence Support Team Brief."

9. *Ibid.*

10. *Concept of Operations,* p. 3.

11. Operation UPHOLD DEMOCRACY, *An Assessment of Intelligence and Communications Systems and Networks* ; Washington, DC, Office of the Assistant Secretary of Defense, 1 December 1955; pp. 1-2.

12. *Ibid.*, pp. 4-23.

13. Operation JOINT ENDEAVOR, Joint Universal Lessons Learned, Draft, 30 January 1997, Lt. Cdr. Paul Jaeger, USN, p. 2.

14. Operation JOINT ENDEAVOR, Joint Universal Lessons Learned, Draft, 7 February 1997; Lt. Col. Ives, USA, p. 1.

15. The NIST in Riyadh, Saudi Arabia, deployed in 1992 in support of Operation SOUTHERN WATCH. It is still operating. Until recently, four other NISTs were deployed in support of Operation JOINT GUARD: Naples (which closed on 1 April 1998) and Vicenza (which closed on 24 May 1998), Italy; Sarajevo and Tuzla, Bosnia and Herzegovina.

16. Twelve NMIST (the NIST's predecessor) teams were deployed in support of Operations DESERT SHIELD and DESERT STORM.

17. Mark Lowenthal, lecture presented to the Joint Military Intelligence College, Washington, DC, 9 May 1998.

18. General Zinni, USMC, lecture presented at CIA, Office of Military Affairs, Langley, VA. Videotape, no date.

19. National Intelligence Support to Join Operations, Joint Pub 2-02, Appendix C.